Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2020. Vol. 14(2): 433–459. DOI: 10.5281/zenodo.4769989
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns

Troy Smith[1]
University of Trinidad and Tobago, Trinidad and Tobago

Nikolaos Stamatakis[2]
United Arab Emirates University, United Arab Emirates

Abstract

For the last twenty years, there has been an increase in literature on cybercrime due to growing awareness of its impact and economic cost. This literature is filled with debate by authors over the correlation between what has been dubbed cybercrime and 'terrestrial crime'. Some have claimed that although cybercrime may be a new and distinctive form of crime in principal, it remains essentially like traditional crime. This argument suggests that traditional offenders have merely adjusted their tactics to utilize the advantages that cyberspace offers. However, other scholars argue that the uniqueness of the cyber environment creates key differences between cybercrimes and traditional crimes. These discrepancies can affect the applicability of general criminological theories previously used to explain terrestrial crimes. This research aims to identify the theoretical concerns surrounding the applicability of the Routine Activity Theory (RAT) of crime in cyberspace, highlighting the practical issues related to such application. Prior to this, the present study seeks to define "cybercrime", as well as provide a comprehensive description of RAT, emphasizing on the correlation between these two concepts.

Keywords: Crime; Cyberspace; Routine Activity Theory; Spatial Distribution.

Introduction

Due to the increasing social, psychological and economic effects of cybercrime, research and supporting literature by social scientists has also increased over the last 20 years (Lee & Alshalan, 2005; Marcum, Ricketts & Higgins, 2010; Bossler & Holt, 2014; Reyns, Fisher, Bossler & Holt, 2018; Kranenbarg, Ruiter & van Gilder, 2019). Although inroads have been made into understanding cybercrime there remains considerable uncertainty and debate with regards to several aspects of cybercrime including typologies and the true nature of cybercrime (Grabosky, 2001; McGuire, 2007; Choi & Lee, 2017). First, numerous taxonomies for cybercrime have been proposed by researchers with

[1] University of Trinidad and Tobago, Trinidad and Tobago.
Email: troy.smith078@we.utt.edu.tt

[2] United Arab Emirates University, United Arab Emirates. Email: n.stamatakis@uaeu.ac.ae

different backgrounds and areas of specialization using different definitions for cybercrime as the base for classification (Fafinski, Dutton & Margetts, 2010; Ghernouti & Simms, 2014). Second, there is a heavy debate about the congruency between cybercrime and 'terrestrial' crime and hence the applicability of traditional crime theories (Grabosky, 2001; Yar, 2005; Bosler & Holt, 2014). Empirical research testing the applicability of traditional crime theories has focused on the use of Routine Activity Theory (RAT) and have had mixed results (Bossler & Holt, 2014; Ilievski, 2016; Reyns et al., 2018). Therefore, to date there remains an absence of a decisive explanation to the congruency of cybercrime to traditional crime.

This study argues that concepts of time and space in cyberspace make it unique and limit the usability of traditional crime theory such as the RAT, which is demonstrated by the inconsistency in the results of previous empirical studies. The present study aims to gain insight into the usability of the RAT to explain cybercrime and the relationship between cybercrime and traditional crime by investigating the predictors of four types of cybercrime victimization/experiences separated into pairs using a binary classification for cybercrimes, for example, Cyber-dependent (techno-centric/computer-based) and Cyber-enabled (people-centric/person-based). Furthermore, seeking to contribute to the current pool of knowledge this study also examines the applicability of the RAT to cybercrime and develop risk models for four forms of cybercrime. It demonstrates the effect of cyberspace on the usability of RAT and by extending the level of congruency between cybercrime and traditional crime. The following sections provide an overview of cybercrime followed by an analysis of the Routine Active Theory (RAT) underlying any special consideration of applying RAT to crime in cyberspace.

Overview of Cybercrime

Technology over the last several decades has become integrated into every aspect of life revolutionizing the way we communicate, bank, shop and how we control aspects of critical infrastructure (Bossler, Burgess & Holt, 2016; Sarre, Lau & Chang, 2018; Bossler & Berenblum, 2019). More than half of the world's population have Internet access and governments continue to increase accessibility to the Internet and technology to their citizens (Schwab, 2019; We Are Social, 2019; United Nations Conference on Trade and Development [UNCTAD], 2019). Ngo and Jaishankar (2017) indicate that there is evidence, which includes a 1998 United States Department of Commerce report that the Internet adoption rate doubles every 100 days. Kokkinos and Saripanidis (2017) indicated that online communication platforms especially Social Network Sites are gaining popularity particularly among adolescents due to low cost and interactive nature. However, regardless of its benefits technology is still only a tool in the hands of the user and like all tools it can be used to build or destroy (Nurse, 2018).

Mendez (2005) anticipates that as access to technology, integration and Internet usage increases that almost all crimes of the future will unavoidably have a cyber component. Nurse (2018) and Coffey, Haveard and Golding (2018) have a suggested that cybercrime rates have run parallel to the increased utilization of the Internet and adoption of technology. In 2016 and 2018, the Office for National Statistics reported that the Crime Survey of England and Wales indicated that cybercrime accounted for more than half of the reported instances of crime for the twelve-month reporting period (Nurse, 2018). In 2013, the United Nations Office on Drugs and Crime released the result of the Comprehensive Study on Cybercrime, in which it indicated that a comparison of cybercrime and conventional crime victimization rates for 21 countries showed that the prevalence of cybercrime victimization had surpassed conventional crime (Malby, 2013). Tcherni, Davies, Lopes and Lizotte (2016) reported that that available global data indicated that the cybercrime rate was increasing and that it was inversely proportional to the rate of traditional crimes.

Although there is not a comprehensive globally accepted value of financial loss associated with cybercrime, the available reports and data sources suggest that it is valued in the billions of US dollars and is increasing each year (Ali et al., 2017; Lewis, 2018; Ponemon Institute & Accenture Security, 2019). Cybercrime does not discriminate and the losses associated have been spread across a variety of industries. In 2012, the financial impact was already being examined and identified as a growing problem with Keith Alexander head of the National Security Agency and U.S. Cyber-Command indicating a forty-four (44%) percent increase in cyber-attacks in the period of only one year and that based on information accessible to him that the financial loss due to cybercrime now accounted for "greatest transfer of wealth in history" (Rogin, 2012; Henney, 2018). Research by IBM using data from 350 companies in 11 countries show a twenty-three (23%) percent increase total cost of data-breaches between 2013 to 2017. In 2017, Symantec Corporation reported that cybercrime had a global cost of USD 100 billion per year (Ali et al., 2017; Ngo & Jaishankar, 2017). However, other reports by the Center for Strategic and International Studies estimate that the global cost of cybercrime may be actually as high USD 600 billion (Center for Strategic and International Studies, 2018). Cybersecurity Ventures and Herjavec group (2019) with support from Frank Abagnale a world-renowned authority on financial crime and FBI consultant have predicted that cybercrime cost will be in excess of USD 6 trillion by 2021. While the estimates vary possibly partially due to the range of classifications of cybercrime differing by jurisdiction and possible under reporting, what can be seen is that cybercrime and its associated cost is increasing rapidly (Ngo & Jaishankar, 2017).

Recently several studies and reports have highlighted the need for a human-centric approach to cybersecurity recognizing the human element as an essential element in the disruption of cyber threats (Leukfeldt, 2017; Deibert, 2018; Back & LaPrade, 2019; Jalkanen, 2019; García-Segura, 2020). Existing literature suggests that the end user is considered the weakest link in cybersecurity because humans want to trust humans and are hence often easily manipulate and deceived (Conteh & Royer, 2016; Ani, He & Twari, 2018; Piper, 2019; Ponemon Institute & Accenture Security, 2019). Human-centric attacks based on social engineering such as phishing have been reportedly so successful and frequent that an international consortium called the Anti-Phishing Working Group was established to mitigate the threat (Anti-Phishing Working Group, 2017). Furman, Theofanos, Choong and Stanton (2011) opine that many users are concerned about cybercrime and cybersecurity but lack the knowledge of threats and protective methods. Recent research has shown that end user activities in cyberspace and online social environments substantially influence the nature of cybercrime victimization (Lee, Choi, Choi & Englander, 2019; Lee & Downing, 2019). Therefore, current data supports the call for a human-centric approach to cybersecurity and exploratory research to provide scholarship that can aide the development of security strategies based on human and social factors. Recognizing the importance of the individual in developing plans to increase cybercrime resilience several groups and researchers have proposed human-centric research agendas and created new yearly conferences focused on the topic (Liaropoulos, 2015; Leukfeldt, 2017; Deibert, 2018). In April 2019, during the opening of the Forcepoint[3] Cyber Experience Center in Boston, the company's CEO Matthew Moynahan and Michael Rogers, former director of the National Security Agency[4] highlighted the need for a greater emphasis on the human aspect of cybersecurity and the development of strategies for more resilient end users (Roy, 2019). Research on the human factor in cybercrime and cybersecurity is essential for policymakers to switch from being reactive to proactive and thereby focus on understanding and preventing incidents rather than stopping incidents (Leukfeldt, 2017; Deibert, 2018; Back & LaPrade, 2019; Roy, 2019).

Conceptualizing Cybercrime

Criminals have followed the world into the digital realm and as a result, they have expanded their reach and repertoire of criminal activity by exploiting the unique opportunities created by technology leading to what is now commonly termed cybercrime (Furnell, 2002; Cross & Shinder, 2008; Choi & Lee, 2017; Bossler & Berenblum, 2019; Piper, 2019). Cybercrime is a therefore a very broad term as it includes both crimes where technology is used or targeted as part of the criminal event (McGuire & Dowling, 2013; Holt, Bossler & Seigfried-Spellar, 2018; Bossler & Berenblum, 2019; Piper, 2019). An analysis of the available literature reveals over 30 different types of offenses that have been classified as cybercrime, which include hacking, online fraud, phishing, cyberbullying, cyberstalking, Denial of Service attacks, spamming, malicious communication, sexting and dating scams (Yang, 2011; Ngo & Jaishankar, 2017).

To date there is no universally accepted definition of cybercrime (Shinder, 2011; Kirwan & Power, 2014; Ngo & Jaishankar, 2017; Sarre, Lau & Chang, 2018; Piper, 2019). However, a for the person of this article a merged definition consistent of the main concepts from various scholars and institutions is provided. Cybercrime is an act that violates the law, which is perpetrated using information and communication technology to either target networks, systems, data, websites and/or technology or facilitate a crime (e.g., Goodman & Brenner, 2002; Wall, 2007; Wilson, 2008; Maras, 2014; Maras, 2016). The definitions differ based on the person's or entity's academic area of focus, available data, geographical location, nature and role of the entity, and whether the focus is to be placed on the victim or the offender (Gordon & Ford, 2006). As a result, some definitions are broader than others. Gordon and Ford (2006), for example, define cybercrime as "any crime that is facilitated or committed using a computer, network or hardware device." Cybercrime can also be defined as a crime involving a computer and a network, while computer crime involves only a computer (Moore, 2011). Both of these definitions are broad; however, the latter goes further by differentiating cybercrime from computer crime.

Many definitions have been designed to highlight the differing level of involvement of cyber-technology in various cybercrimes (i.e. highlighting crimes that use cyber-technology and crimes that depend on cyber-technology) (Cross & Shinder, 2008). Some

[3] Forcepoint, is an Austin-based company owned by U.S. defense contractor Raytheon and private equity firm Vista Equity Partners. It develops and markets cybersecurity software including firewall, cloud access, cross-domain IT security products and insider threat solutions.

[4] The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes.

definitions focus on identifying the type and degree of involvement of cyber-technology required for a specific criminal activity to be denoted as a cybercrime. One such definition defines cybercrime as "a criminal act in which a computer is used as the principal tool" (Forester & Morrision, 2001). Some researchers have also attempted to include criminological theory into their definitions. Several writers have described cybercrime as an invasion of computer or network systems to achieve criminal ends or use of computers as instruments of crime, given that the 'guardians' lack the resources or knowledge to prevent or detect the crime (Wilson & Kunz, 2004; Gordon & Ford, 2006; Jahankhani & Al-Nemrat, 2010).

The difficulty associated with defining cybercrime can be attributed to a lack of tangible statistical data on crimes that use cybertechnology (Cross & Shinder, 2008). This shortage of data can be attributed to a lack of reporting by individuals to Law Enforcement and the disconnect between Law Enforcement and the persons or bodies that collect and utilize such statistics. The underreporting is also attributable to police not being viewed as experts in the arena of cybercrime, little prospect of restitution or compensation and possible embarrassment (British Crime Survey, 2004; Wall, 2007; Jahankhani et al., 2014). There is also underreporting due to persons not being aware of becoming a victim (Jahankhani et al., 2014). This can be true in cases of Advance Persistent Threat[5] (APT) and malware, which act as keyloggers[6] or covertly control computers for use in botnets[7]. Cross and Shinder (2008) suggest that based on their experience it may be near impossible to acquire an accurate count of cybercrimes from the police.

Besides its complication, the definition of cybercrime is essential in its study as it defines the range of activities of which it comprises and forms the base for any classification system. Further, at the macro level a unified definition that clearly defines the range of illicit activities, which can be termed cybercrime, can have several benefits. First, a clear operationalized definition for cybercrime is essential in any research to enable continuity and comparison of research International Telecommunications Union, 2012; Mowery, 2013; Warf, 2018). Second, it provides a common language essential to collaboration and meaningful discussion (International Telecommunications Union, [ITU] 2012; Mowery, 2013; Warf, 2018). Third, it also guides the methodology as it relates to the types of crime which will be measured and which crimes can be grouped i.e. it defines the scope of the project International Telecommunications Union, 2012; Mowery, 2013; Warf, 2018). This researcher proposes that testing of the classification empirically to determine if the crimes follow a similar pattern in reality, which can aide in filtering out or refining present definitions and typologies.

Classification of Cybercrime

[5] A cyber-attack in which an unauthorized person gains access to a network and stays there undetected for an extended period. The aim of an Advance Persistent Threat attack is to steal data rather than to cause damage to the network or organization.

[6] Malware that records keystrokes made by a computer user, generally to gain fraudulent access to passwords and other confidential information.

[7] A network of private computers infected with malware and controlled as a group without the owners' knowledge, e.g., to send spam messages.

The varying definitions of cybercrime and focus of researchers due to differing academic background and goals have led to numerous proposed taxonomies (Wall, 2007; Choi, 2018; Madriaza & Palacio, 2018). These taxonomies are based on factors such as, target, technological dependence, classes of offenders, method/tool used, degree of penetration, and motives (Rogers, 1999; 2001; 2006; Chakrabati & Manimaran, 2002; Sukhai, 2004; Krone, 2005; Hansman & Hunt, 2005; Kanellis, Kiountouzis & Kolokotronis, 2006; Thomas, 2006; Williams, 2008; Meyers, Powers & Faisol, 2009; Poonia, 2014; Ibrahim 2016). Some are hybrid to create classifications that are more intricate. Among the existing taxonomies there are varying levels of overlap, however, there remains considerable differences in contents, definition and structure (Ghernaouti & Simms, 2014). Somer (2019) indicates that there continues to be no consensus on the best approach to development a single taxonomy of cybercrime. However, technology-based taxonomies have emerged as the most dominant (Wall, 2001; 2007; 2017; Yar, 2006; Urbas & Choo, 2008; Ghernaouti & Simms, 2014; Jahankhani et al., 2014; Choi, 2018).

The overlap of classifications is seen particularly in the extant literature, which categorizes cybercrime based on the computer's relationship to the crime i.e. technology based taxonomies. The most well-known of which is Wall's (2001) early three-category typology, which divides cybercrimes into the following categories: cyber-trespass (e.g. hacking), cyber deception and theft (e.g. identity theft), cyber-porn and obscenity (e.g. exploitation) and cyber-violence (e.g. cyberstalking) (Madriaza & Palacio, 2018). This typology by Wall (2001) can be simplified as crimes in the device, crimes using the device and crimes against the device (Wall, 2007; Madriaza & Palacio, 2018). Crimes in the device relate to where the devices' content is prohibited or illegal and can lead to violence or hate crimes. Crimes using the device apply to crimes where technology is used to engage and or deceive the intended victim i.e. crimes against the individual (Wall, 2015). The final category of crimes against the device relate to situations where the device, system or network are compromised by directly attacking the factors of Confidentiality, Integrity and Availability, which is collectively called the CIA triad (Mohanty, Ganguly & Pattnaik, 2018; Madriaza & Palacio, 2018). Yar (2006) later added a new type of activity to the four above, which is 'crime against the state'. 'Crimes against the state' are those activities that threaten the integrity of a nation's infrastructure such as, (cyber) terrorism, (cyber) espionage and disclosure of official secrets (Yar, 2006). Another taxonomy categorizes cybercrime in terms of the specific role of the computer in the crime: crimes where the computer is the target; crimes where a computer is the medium (Urbas & Choo, 2008); and crimes where the presence of computers is incidental (Goodman, 1997).

Building on Wall's (2001) four-category typology, a new taxonomy later emerged which expresses cybercrimes in terms of differing relation to a terrestrial crime or the importance of cyberspace in their execution. This taxonomy drew on the precedents of criminal justice and suggests that computers are a tool that facilitates terrestrial crimes, making cybercrime a new category of traditional crime rather than a new area (Wall, 2005; 2007). This new taxonomy classifies cybercrimes into three categories: 1) Computer-assisted crimes - traditional crimes adapted to be committed through cyberspace; 2) Computer content crimes - partially new crimes, which are known crimes that are modified to better correspond and react to the new media; and 3) Computer integrity crimes - new crimes that have been made possible by the existence and scope of cyberspace (Ghernaouti & Simms, 2014; Ibrahim, 2016). These categories can be matched to Wall's (2005) categories of cybercrime: computer-assisted crimes (cyber deception and theft); computer integrity crimes (cyber-trespass); computer-content crime I (cyberporn and obscenity); and computer-content crime II (cyber violence) (Jahankhani et al., 2014).

There are also several binary technology-based classification models, which classify cybercrimes specifically on the degree of involvement of cyber-technology (Ghernaouti & Simms, 2014). These models focus on the psychological principle of categorization and provide a simplified method of delineating the nature of specific cybercrimes. One of the first proposed binary models classified cybercrimes into, techno-centric (Type I) and people-centric (Type II) (Gordon & Ford, 2006). In this model, Type I and Type II crimes are at the two extremes of a continuum which dichotomizes cybercrimes based on the degree of involvement of the cyber-component versus the people-component of the crime (Ibrahim, 2016). Closely related to the techno-centric and people-centric classifications are the classifications of cyber-enabled crime and cyber-dependent crime (McGuire & Dowling, 2013). Cyber-enabled crimes are crimes which can be committed without the use of cyber-technology (i.e. they are not dependent on cyber-technology and can be executed independently in the physical world); while cyber-dependent crimes are those which can only be committed using cyber-technology, such as computers or computer networks. While using the same designations of Type I and Type II as Goodman (2007), some researchers have also taken a slightly different approach to classification by basing theirs on the role of the computer in the crime (Alkaabi, Mohay, McCullagh & Chantler, 2010). More recently in 2014, a new binary model was proposed, which suggests two general categories simply identified as active and passive computer crimes (Jahankhani et al., 2014). An active computer crime is defined as criminal activity in which a computer is used to commit the crime and a passive computer crime occurs when a computer is used to both assist and advance/exacerbate an illegal activity. Tavani (2001, 2013) takes a similar approach to classify cybercrime by first defining a 'genuine' cybercrime as, "the criminal act can be carried out only using cyber-technology and can take place only in the cyber-realm". This idea of defining a 'genuine' cybercrime by highlighting the need for cyber-technology to be the main tool or rather an irreplaceable part of the crime is shared by Forester and Morrison (2001) and Girasa (2002). Additionally, Tavani's taxonomy classifies other crimes involving cyber-technology that are not genuine cybercrimes, which fall under broader definitions of cybercrime as cyber-related crimes. These distinctions differentiate between a crime in which cyber-technology is mandatory for its execution from crimes which are enhanced by computers and cyber-technology but can occur without its presence (Cross & Shinder, 2008; Jahankhani et al., 2014; Choi, 2018). However, it is believed that these binary models – while useful in analyzing voluminous cybercrime variances – fall short in differentiating between cybercrimes by motivation and as such are better as explanatory tools (Ghernaouti & Simms, 2014).

There have been several other novel taxonomies proposed by researchers, which took a target-centric, legal, motivational or multi-lens perspective. One target-centric taxonomy categorizes cybercrime in terms of the specific role of the computer in the crime: crimes where the computer is the target; crimes where a computer is the medium; and crimes where the presence of computers is incidental (Goodman, 1997). Subsequently, other taxonomy were proposed, which used a similar rule for classification with only two categories: crimes where computers systems are the target; and crimes where the computer is the medium (Urbas & Choo, 2008). Several researchers have identified other factors along which to classify cybercrime leading to proposal of their own unique taxonomies

(Land et al., 2013; Ibrahim 2016; Agrafiotis et al., 2018). The legal perspective for classification can be seen in the works of Mali (2009) and Kota (2015), which defined cybercrime classes based on legally defined targets: 1) Cybercrime against the Individual, 2) Cybercrime against Property and 3) Cybercrime against Organisation or Society. Ibrahim (2016) proposed a taxonomy based on tenets of motivational theories leading to three classes of cybercrime based on the main motivation of the offender; socioeconomic, psychosocial and geopolitical. Recently multi-lens or hybrid taxonomies have also emerged such as Brar and Kumar (2018) who sought to combine principles of cybersecurity and cyber incident survey data to create a taxonomy that covers all types of cyberattacks. The proposed taxonomy divides cybercrimes into four main categories focusing on how they affect/target data Confidentiality, Integrity and Accessibility (CIA Triad); Cyber violence, Cyber-peddler, cyber-trespass and cyber-squatting (Brar & Kumar, 2018). Another hybrid taxonomy was presented by Agrafiotis, Nurse, Goldsmith, Creese and Upton (2018) who sought to develop taxonomy a specific to the target and the impact of the cybercrime i.e. a taxonomy for cyber-harm targeting organisations. This taxonomy divides organisational cyber-harm into the five classes of Physical/Digital, Economic, Psychological, Reputational and Social Societal (Agrafiotis et al., 2018). The previous hybrid taxonomies were limited to two perspectives, however, more recently Donalds and Osei-Bryson proposed what they view as a holistic/multi-perspective approach using several perspectives. The classification model aimed to create a taxonomy that is functional for a variety of cybercrime stakeholders. The taxonomy proposed by Donalds and Osei-Bryson (2019) takes a hierarchal approach that considers the attacker, complainant, impact, location, target, tool and technique, victim and the vulnerability exploited.

Counter to the efforts of the above researchers, other scholars view the attempt to establish a taxonomy of cybercrime as an exercise in futility (Fafinski et al., 2010; Ghernaouti & Simms, 2014). Cybercrime and its associated behaviour are outside of the boundaries of criminal law and that the threat vector used and/or target are immaterial (P. Somer cited in Fafinski et al., 2010). Ingraham (1980) originally expressed this belief when discussions on the meaning of computer crime first started. Similar thoughts to Sommer and Ingraham have been expressed by Easterbrook (1996) comparing the development of cybercrime taxonomy to taxonomy on 'horse law', which would be shallow missing unifying principles. He expressed what he believes to be the trivial nature of creating a new taxonomy for something that should be brought to mesh with current legal frameworks. However, this argument has met objection and countered by highlighting the need for the law to continue to evolve as environments change; and that cyber-law would need to be continually reassessed as cyberspace continues to grow and develop (Lessig, 1999).

The literature provides an array of classification strategies related to cybercrimes, however, the majority in their simplest form group the crimes based on the role/dependency/importance of technology in the execution of the crime. This is important as it demonstrates a recurring theme of technology's defining role in cybercrime and the possible proportional nature of technology to the nature of specific cybercrimes. The range of cybercrimes generally fit into two categories: crimes where a computer or network is the target of the crime or crimes in which the computer is used as a tool to facilitate traditional criminal activities i.e. crimes that may occur in the absence of technology (McGuire and Dowling, 2013; Europol, 2018, p.15; Piper, 2019; United

Nations Office on Drugs and Crime, 2019). The key distinction between the aforementioned classes of cybercrimes is the role of technology in the offence - whether it is the target of the offence or part of the modus operandi of the offender (United Nations Office on Drugs and Crime, 2013).

The Routine Activity Theory (RAT)

Following the conceptualization and classification of cybercrime, this section seeks to underline the relevance of RAT in terms of cybercrime, as the identification of factors leading to an increased probability of predation through Routine Activities Theory (RAT) has a significant part in the study of criminology and victimology (Holtfreter et al., 2008; Reyns et al., 2011; Pratt et al., 2013). Routine activity theory is a sub-field of rational choice theory, which was developed by Marcus Felson and Lawrence Cohen, which has been applied to a range of victimization experiences (Holtfreter, Reisig, & Pratt, 2008; Breetzke & Cohn, 2013; Argun, & Dağlar, 2016; Leukfeldt & Yar, 2016; Louderback & Roy, 2018). Routine activities can be defined as, generalized temporal and spatial patterns of recurrent and prevalent social activities which provide for basic population and individual needs, whatever their biological or cultural origins generalized patterns of social activities in a society (Cohen & Felson, 1979; Bock, Shannon, Movahedi & Cukier, 2017; Wikström, Mann & Hardie, 2018). RAT seeks to understand the personal and situational aspects of victimization (Schreck & Fisher, 2004; Schreck, Stewart & Fisher, 2006; Holtfreter et al., 2008; van Wilsem, 2011, 2013).

the Routine Activities Theory provides a macro perspective predicting how changes in social and situational conditions influence the probability of a crime event and victimization rate (Cullen & Agnew, 2006; Stein 2011; Howell, Burruss, Maimon & Sahani, 2019; de Jong, Bernassco & Lammers, 2019). This suggests that crime is a non-accidental/non-random phenomenon. The combination or convergence of a motivated offender, an attractive target and a lack of capable guardianship these elements provides an opportunity for criminal or deviant activity and therefore the propensity for some to exploit this opportunity. This, in turn, increases both the risk of victimisation and actual victimisation rates (Cohen & Felson, 1979; Yar, 2005; Cullen & Agnew, 2006; Miró-Linares, 2013; Kringen & Felson, 2014). As such, events that cause an individual to spend more time in a public domain increase the probability of victimization (Cohen & Felson, 1979).

Special Considerations of Applying RAT to Crime in Cyberspace

The explanatory schema of RAT is based on the presupposition that the spatial and temporal variables, which define persons, objects and activities, are essential predictors to successful criminal events (Yar, 2005). As a sub context to spatial consideration, there is a positive correlation between proximity to a high concentration of potential offenders and probability of victimization (Cohen, Kluegel & Land, 1981; Miethe & Meier, 1990). Overall, the theory depends on being able to define specific places and the temporal order of activities, which leads to the convergence of target and offender. When applying RAT to cyberspace, the routine activities of interest are online activities including online communications, shopping, business transactions, environments, and sites visited. Additionally, attention is paid to the quantity and type of information which potential victims place online. However, there is a requirement for the proximity between target and offender to be measurable. The transfer of RAT to cybercrime requires that in cyberspace' place, proximity, distance and temporal order be identifiable and definable as in the 'physical world'.

From a theoretical viewpoint, consideration of the applicability of conventional crime theories to cybercrime is affected by two disputes surrounding cyberspace's spatiality and the related topic of cybercrime's congruency to terrestrial crime (Choi & Lee, 2017). On one side, 'Continuists' suggest that cybercrime is not a unique form of crime, rather a conventional crime occurring in a new environment (Grabosky, 2001; McGuire, 2007; Choi & Lee, 2017); while on the other side, 'Transformationists' believe that cybercrime is a new criminality by virtue of the unique properties of the new space in which it occurs (Capeller, 2001; Choi & Lee, 2017). Both views may be true to some degree. Research conducted so far suggests that the organization of crime or variables, which lead to predation, are homologous between the virtual and terrestrial environment (Yar, 2005). However, there are still differences between virtual and terrestrial crimes at the conceptualization level of the variables, which define susceptibility to predation (Yar, 2005). Considering the VIVA model, which identifies Inertia as a property, an inconsistency in conceptualization can be identified. The same physical dimensions do not define cyber targets as terrestrial targets such as weight, which determines difficulty to move and hide the target.

Spatiality in Cyberspace

Theorists and analysts of cyberspace suggest that concepts of proximity, distance, and finite location do not apply to cyberspace, which can be considered as 'anti-spatial' (Mitchell, 1995; Lattimer, 2013; Taylor, Fritsch & Liederbach, 2018). Some geographers share a similar sentiment, as they believe that new social spaces created by cyberspace transformation of space-time relations lack the formal qualities of geographic spaces (Adams & Warf, 1997; Kitchin, 1998; Kitchen, 2009). The virtual environment is considered one in which points are co-present (i.e. space between them can be considered as zero) (Stalder, 1998). This means cyberspace is non-metric and entities or events cannot be meaningfully defined in terms of spatial contiguity, proximity and separation; and as such, space is discontinuous with the terrestrial world (Capeller, 2001). Consequently, the geographical factors of distance and topology that can act as barriers to social action and interaction are negated (Dodge & Kitchin, 2001: 62).

Additionally, the Internet has created "spaceless, placeless" social spaces where people interact but not parallel space-time relations of terrestrial interactions (Kitchin, 1998). Exacerbating this problem, spatiality in non-virtual and virtual environments could have different levels of stability. The non-virtual environment is relatively stable with generally incremental change in the organization of entities in its infrastructure (Yar, 2005). This socio-spatial stability allows ecological approaches to crime analysis, such as RAT, to correlate crime predation to sociodemographic factors and associated routine activities. However, virtual environments are extremely malleable, and changes can occur in seconds. Virtual architecture and topologies offer little resistance to change. In an environment, which may be considered anti-spatial, this instability increases the difficulty of using a theory based on spatial convergence.

Irrespective of these issues, there has been some theorization of at least partial convergence between spatial properties of cyberspace and the terrestrial environment (Kitchin, 1998; Yar, 2005; Rechavi, Bereblum & Maimon, 2015, Song et al., 2016). While cyberspace is considered anti-spatial, online activity is connected to the physical world in two distinctive ways. First, access to cyberspace and the Internet is closely correlated to existing cleavages of income, education, gender, ethnicity, age and disability, and that physical world differences (urban-rural, first world-third world, or low- high income) are translated into cyberspace (Castells, 2002, cited in Yar, 2005). This suggests that socioeconomic differences among individuals affect their ability to access Information and Communication Technologies (ICT), including computers and the Internet (Mossberger, Tolbert & Stansbury, 2003). If demographic factors, like ethnicity, are indeed statistically significant predictors for cybercrime, it stands to reason that location becomes a factor as there tends to be an uneven distribution of these factors within a country (Song, Lynch & Cochran, 2016). Song et al. (2016) work support this hypothesis as the results showed that cyber victimization varied between the use of cyberspace at home vs. outside of the home and between urban and non-urban regional. This was postulated to be related to the type of sites and activities a user would tend to use or feel comfortable using at home in comparison to another location. Urban areas tended to have different economic and educational composition to non-urban regional, which could affect access, types of services available, knowledge of users and time available to spend online.

The five-layer model of cyberspace demonstrates that there is a solid connection between the virtual world and the 'real world' as cyberspace should carry some non-virtual spatial properties into its operations (Rosenzweig, 2013). The two base layers (physical layers) in the model are the 'geographic layer' and the 'network connection layer', which represent the fixed points of data, access, the physical connections between these points and the associated measurable separation between access points (Kitchin, 1998; Rosenzweig, 2013). Though cyberspace itself has no physical existence, each piece of equipment of which it is comprised has a physical location and is linked together across geographic spaces. Therefore, it can be inferred that cyberspace is subject to the control of many different political and legal systems. Furthermore, although in cyberspace movement is seemingly instantaneous making the distance between locations appear to be effectively zero, not all points may be equidistant (Yar, 2005). Therefore, becoming aware of a potential victim's existence or converging with that potential victim may require an offender to spend some time and effort (Yar, 2005).

Explanation of Cybercrime Through Spatial Analysis

In the traditional application of the RAT, successful predation requires the alignment of a motivated offender with a suitable target and a lack of suitable guardianship at a particular location and time. This is described as the spatio-temporal accessibility of the target, which is essential for the crime to take place (Yar, 2005; Reyns et al., 2011; Reyns, 2013). The ontology of the terrestrial world helps to effectively calculate the likelihood of convergence between offenders and their prospective targets as it allows for measurement of proximity and distance. However, the spatial diversity or rather the lack of a clear ability to assign a geographic location to incidents or activities in cyberspace have made researchers hesitant to use spatial analysis in cybercrime research (Goodman & Brenner, 2002; Brenner, 2004; Yar, 2005; Wall, 2007; Ilievski, 2016). Cyberspace is often seen as a barrier to the application of the RAT as a key requirement of the theory that the suitable target and the motivated offender must converge in space (Yar, 2005). This is because cybercrimes can occur without a suitable target and the motivated offender occupying the same physical space or even the same country. In other words, cyberspace does not exhibit a spatio-temporal ontology congruent to the physical world; and hence, cyberspace could be described as "chronically spatio-temporally disorganized" or "anti-spatial" (Vakhitova, Reynald & Townsley, 2016). This spatial disconnect in cyberspace means that the viability of RAT as an etiological model for cybercrimes would be questionable, given the model's dependence on the ability to identify convergence and divergence, proximity and distance, to explain the probability of predation (Yar, 2005).

So, what would happen if online-places (e.g., social networking sites) were considered as the equivalent of physical places? The problem of physical proximity to suitable targets in cyberspace would be neutralized, considering the spatiality of cyberspace as a "systems' problems" (Newman & Clarke, 2003; Reyns et al., 2011). This concept can be understood by comparing cybercrimes to terrestrial crimes in which victim and offender are not in the same physical location, such as fraud associated with a telecommunications system or a mail/parcel delivery system (Reyns et al., 2011). In both cases, although victims and offenders do not intersect at the same physical location, they do converge within a system of networked devices. This suggests that redefining convergence and the role of the physical environment in cybercrime may neutralize the problem of spatiality in cyberspace. Therefore, a better operational definition for the theoretical framework of the RAT may then be: "Opportunities for victimization are created when motivated offenders and suitable targets intersect in environments lacking capable or effective guardianship" (Reyns, 2015: 399). This definition implies that adapting the RAT, to reconcile with the inconsistency in the spatiality of cyberspace vs terrestrial, would lead to its ability to explain victimization in cyberspace (Tillyer & Eck, 2009 cited in Reyns et al., 2011). However, while Yar (2005) makes a convincing case for connecting cyberspace to the physical world, it is not sufficient to provide a clear understanding of how proximity between offender and target in cyberspace can be reconciled to fit the RAT (Yucedal, 2010). Rather, the arguments may better explain differences in the RAT concept of target suitability, as it can be seen how physical/spatial factors can affect access and type of device used by individuals (Yucedal, 2010).

At the same time, there is a dearth of attempts to define cybercrime in terms of spatial distribution with this researcher only finding one article which was published in India by Saravanan and Thilagaraj (2014). In the past, other researchers have chosen to take a less direct approach to include some spatial aspect into their research. For instance, the spatial patterns of 'location of Internet access'; were used to define the spatial aspect of online activities (Song et al., 2016). Research of this type found that the time spent shopping and banking online is longer at home than at other locations (Ren et al., 2013). This can be compared to previous research, which has shown that shopping and banking online increase the risk of cyber-theft victimization (Pratt et al., 2010; Reyns, 2013; van Wilsem, 2013). Saravanan and Thilagaraj's (2014) research sought to predict cybercrime prone regions and trends in geographic-based locations in relation to nine different types of cybercrimes in India using datamining techniques, which were subsequently visualized using Geographical Information Systems (GIS). Comparison of these two sets of results suggests some correlation between where the Internet is accessed, the purpose for accessing the Internet and the duration of the access. This means that a person using the Internet at home may expose himself or herself to a greater risk of victimization through increased time spent engaging in risky online activities.

Demographics and Cybercrime

There is a structural dimension in the theoretical perspective of routine activity theory (Cohen, Felson & Land, 1980). In conventional crime, it has been proposed that structural dimensions define structural opportunity (Cohen & Felson, 1979); and when the spatial aspect of RAT is examined the importance of demographic characteristics are elucidated (Hindelang et al., 1978). Structural opportunity refers to conditions, which do not necessarily cause an event e.g. crime but rather creates an environment in which it can occur. Structural factors that lead to structural opportunities encompass macro-level factors, such as socioeconomic, legal and political factors (Messner & South, 1992; Press, 2016; United Nations Office on Drugs and Crime, 2018). Demographic characteristics such as employment and level of education influence behaviour and role expectations. Furthermore, demographics affect the type and level of involvement in various activities by individuals. The resulting concert of activities that form the lifestyle of the individual determines the probability of victimization as it affects the chance of spatio-temporal convergence between a motivated offender and a suitable target (van Wilsem, 2002, 2003; Stein, 2010). While the virtual environment itself is not bound to traditional spatial concepts, access is controlled by terrestrial constraints. Access cyber-technology/online resources follow existing lines of social inclusion and exclusion with its use being dependent on factors such as income, education, gender, ethnicity, age and disability (Castells, 2002: 247-256). Consequently, presence and absence in the virtual world translate to 'real world' marginalities, which themselves are profoundly spatialized.

Also, what is accessed can be dependent on spatial factors, as information usefulness depends on the locale of the user (Kitchin, 1998). The cultures within different communities vary and translate into people in each geographic location having unique beliefs, desires, and expectations. This results in various specific online routines and behaviours being associated with or limited to various geographical boundaries, suggesting that the online density and activity of both potential offenders and targets are dependent on the distribution of the resources and skills needed to be present and active in cyberspace (Yar, 2005). The linkage between cyberspace and terrestrial space through the geographies of data, hardware and connections may also negate the perception of instability. This means that the online content and access points (websites) may change, the hardware remains relatively constant and extend into cyberspace through for example Internet Protocols (IP) addresses.

Temporality in Cyberspace

The ability to locate targets at specific locations at set times is a basic presupposition of RAT. Routine activities should exhibit a clear temporal sequence and order. Except for opportunistic crimes, the offender tends to actively seek to increase the probability of predation by attempting to engage in a criminal event when they know or predict the spatio-temporal accessibility of targets (Felson, 1998; Moise, 2014).

There exists a temporal aspect to the use of cyber technology and more specifically the Internet. However, time in cyberspace is not necessarily a supplementary variable that can account for simultaneity. It is important to understand this temporality when applying RAT as it reveals the correlation between time and social interactions in cyberspace (Dodge & Kitchin, 2003). Charting of the daily and hourly cycles of users of Usenet, as shown in Figures 1. & 2., demonstrate the temporality of posting with a clear illustration of the peaking of activity and specific periods (Smith & Kullock, 1999). These peaks above coincide with geographic space. For example, early morning on the East Coast of the US coincided with mid-afternoon in Europe (Smith, 1999). These can be tied to daily fluctuations in Web usage and data transfer rate changes or delays at different periods (Dodge & Kitchin, 2003).

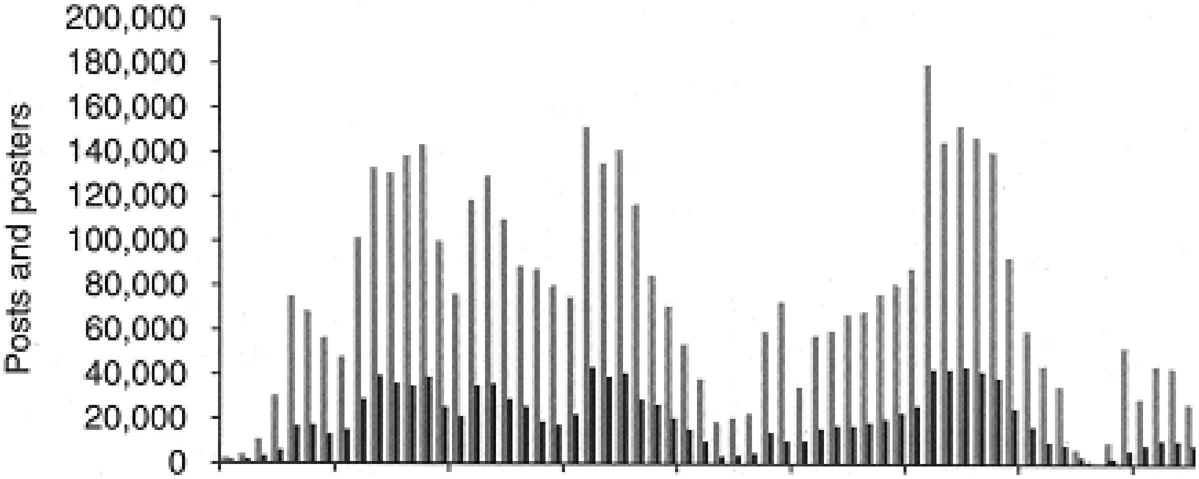

Figure 1. Daily rates of messages and participants in Usenet, 1 November 1996 to 12 January 1997. Reprinted from "Mapping Information and Communication Technologies" by M. Dodge and R. Kitchin, Mapping Cyberspace, 2003, London, UK: Routledge. Released under Creative Commons license, 2017

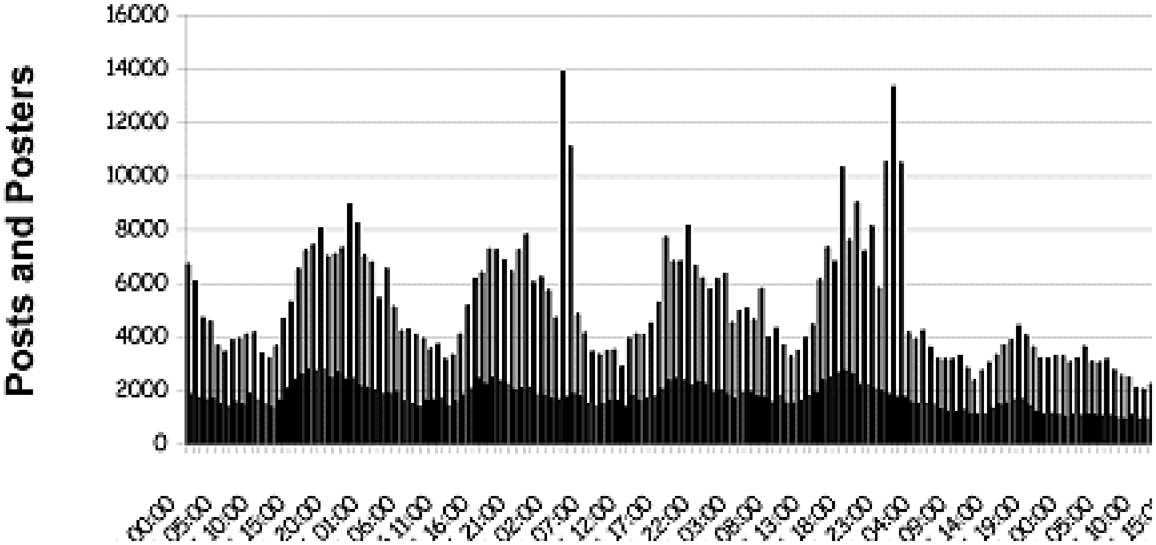

Figure 2. Hourly rates of messages and participants in Usenet, 12 November 1996 to 18 November 1996. Reprinted from "Mapping Information and Communication Technologies" by M. Dodge and R. Kitchin, Mapping Cyberspace, 2003, London, UK: Routledge. Released under Creative Commons license, 2017

Time in cyberspace can also be defined as the duration of exploration. This is important as the time spent online or on a specific site determines the probability of encounter between a potential target and motivated offender. Time of exploration determines the possibility of encountering an offender 'directly' as in an online chat, limits the amount of information shared online, and determines the potential depth of exploration of a specific website and number of websites visited (Mihalache, 2002). This can be linked indirectly to spatial and temporal factors such as bandwidth, which differs based on location and time of day.

However, in the strict sense cyberspace does not follow a traditional temporal construct. Although there may be patterns in levels of network activity (Smith, 1999), online activities span a variety of locations and motivations and cannot be confined to clearly delimited temporal windows (Yar, 2005). This is further exacerbated by the continuous connectivity that mobile Internet provides (i.e. even if a user may always be connected and/or passively active), information (e.g. location) may still be shared automatically. This poses a specific problem in identifying patterns of convergence between different dimensions of criminal activity.

Discussion and Conclusion

While previous research has undoubtedly provided insight into factors affecting the risk of victimization, there are some shortfalls in methodology and gaps in the literature, as these studies generally tend to focus on only one type of cybercrime (either property, individual, or government). To date, the literature has been limited in country, target population and size of the sample used in the research. The bulk of research has taken place in the United States of America utilizing special samples from isolated colleges or university students, and generally using purposive sampling (Bjerregaard, 2000; Logan, Leukfeldt & Walker, 2000; Fisher et al., 2002; Lee & Alshalan, 2005; Bossler & Holt, 2008; Marcum et al., 2010; Reyns, 2013, 2015). There is a dearth of research recorded outside of the United States of America, with the only other countries recorded being India, Spain, Finland and Nigeria with either special samples being taken from schools and cyber-café users or secondary data being used (Ndubueze, Igbo & Okoye, 2013; Oksanen & Atte, 2013; Alvarez-Garcia, Perez, Gonzalez & Perez, 2015). While there have been several individual studies (Marcum, 2008; Marcum et al., 2008; Ngo & Paternoster, 2009; Bossler et al., 2011; Reyns, 2013) the variety of online activities examined have been limited and may negatively impact the generalizability of the results (Ilievski, 2016). A review of the literature clearly shows an opportunity for expanding current knowledge through modification of pass methodologies in several ways.

First, there is a need for examination of under-studied forms of cybercrime such as malware, hacking and online fraud since focus has primarily been given to person-based forms of cybercrime such as cyber-bullying (Marcum et al., 2010; Moore, Bohme & Riek, 2010, Navarro & Jasinski, 2012) and online harassment (Bossler & Holt, 2009). The insight offered by these studies has also been limited due to limitations in data acquisition and operationalization of crime theories; minimal sampling outside the United States and Europe, samples predominantly taken from college students, bias towards examining interpersonal crimes and crimes often being examined in isolation (Moitra, 2005; Marcum, 2008; Navarro & Jasinski, 2012; Reyns, 2013; Ndubueze et al., 2013, Alvarez-Garcia et al., 2015; Ilievski, 2016).

Second, most studies available have only partially operationalized the theoretical framework of the RAT (i.e. using one or two rather than all three of the concepts of a suitable target, motivated offender and capable guardianship). This has highlighted the ability of the individual latent variables to predict victimization but does not allow insight into how they simultaneously affect the risk of victimization (i.e. accounts for interactions). Cyberspace is a unique environment that essentially creates the opportunity for cybercrime, and as Yar (2015) connotes, the temporal and spatial assumption of the RAT is not easily transposable to cyberspace. These assumptions make the RAT ideal in determining the potential difference between cybercrime and terrestrial crime.

Yet, it can be inferred that if the assumptions do not hold true, it would result in the RAT being inapplicable to cybercrime. If cybercrime is not congruent to traditional crime (i.e. the properties of cyberspace), the ability of the RAT should be limited, as the properties of cyberspace do not align with Yar (2005) theory's core assumptions. Therefore, the usability of the RAT should be markedly different between the two classes of cybercrime but similar within the classes. However, an inconsistent or unpaired outcome would suggest that other factors exist. Further unexpected pairing may suggest that cybercrime may be better classified along the lines of another unidentified variable rather than technology. This research postulates that the degree of involvement of technology/cyberspace determines if or to what degree the assumptions of the RAT holds true. Therefore, RAT should be less applicable to crimes that are more dependent on cyberspace than those which are closer in nature to terrestrial crimes. Despite the possible limitations of establishing guardianship as defined in the terrestrial world, RAT's concept of capable guardianship should be transposable to cyberspace. The difference in structural properties of the environment (such as its variable spatial and temporal topology) may be accounted for by establishing a new conceptualization of guardianship.

Third, there is a need to add credence to observations made bypass researchers into RAT by broadening the range of countries surveyed, increasing the sample size and choosing samples that are more likely to be representative of the target country's population. As the reach of the Internet increases and the targets of cybercriminals become broader, it is important to examine online routines from a variety of countries and groups. This is especially necessary since the aforementioned studies have consistently used non-probability samples and or random sampling with low response rates from special populations limiting the ability to make inferences about trends in the general population. Therefore, further region-specific research could add data and trend analysis for a new environment compared to the data collected in the larger continents with differing social, economic, cultural and legal profiles. The small scope of previous research also requires more study to substantiate the hypothesis that behaviour is more significant than socio-demographic variables in its effect on the risk of cyber victimization.

Fourth, while criminology literature acknowledges that demographic factors are related to general crime victimization in the physical world the same cannot be said for cybercrimes. The relationship between cybercrime and demographic factors have not been highlighted in previous studies, and results have been inconsistent with a small range of demographic factors being considered (Choi, 2011). It will hold the field of victimology in good stead to assess the relationships between demographic variables and cybercrime victimization. Furthermore, there may also exist a statistically significant association between demographic variables and concepts outlined by the RAT, namely digital-capable guardianship, risky online behaviours and deviant behaviours.

Ultimately, there remains a considerable gap in efforts to resolve the dispute between Continuists and Transformationists that based on the relationship between cybercrime and conventional crime. Underlying this argument is the dispute to surrounding the spatiality of cyberspace which theoretical relates directly to the efficacy of the Routine Activity

Theory application to cybercrime as the underlying principle requires the offender and victim to occupy the same space at the same time for a crime to occur. The above continuities, however, do not negate the qualitative differences that intrinsically exist between the spatiality of non-virtual and virtual worlds. These inconsistencies between the virtual and non-virtual environment may require a reevaluation of philosophical and sociological assumptions, which form the base of conventional crime theories when attempting to apply them to cybercrime.

References

Adams, P. C., & Warf, B. (1997). Cyberspace and Geographical Space. *Geographical Review*, *87*(2), 139–145.

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity*, *4*(1).

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services. *International Journal of E-Education, e-Business, e-Management and e-Learning*, *7*(1), 70–78.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, A. (2010). Dealing with the Problem of Cybercrime. *2nd International ICST Conference on Digital Forensics & Cyber Crime*. Abu Dhabi.

Álvarez-García, D., Pérez, J. C. N., González, A. D., & Pérez, C. R. (2015). Risk Factors Associated with Cybervictimization in Adolescence. *International Journal of Clinical and Health Psychology*, *15*, 226–235. https://doi.org/10.1016/j.ijchp.2015.03.002

Ani, U. D., He, H., & Twari, A. (2018). Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workplace. *Journal of Systems and Information Technology*.

Anti-Phishing Working Group. (2017). APWG: Unifying the Global Response to Cybercrime. https://doi.org/10.1109/MSP.2011.180

Argun, U., & Daglar, M. (2016). Examination of Routine Activities Theory by the Property Crime. *nternational Journal of Human Sciences*, *13*(1), 1188.

Back, S., LaPrade, J., Shehadeh, L., & Kim, M. (2019). Youth Hackers and Adult Hackers in South Korea: An Application of Cybercriminal Profiling. *IEEE European Symposium on Security and Privacy Workshops*, 410–413.

Bennett, R. R. (1991). Routine Activities: A Cross-National Assessment of a Criminological Perspective. *Social Forces*, *70*(1), 147–163.

Birkbeck, C., & LaFree, G. (1993). The Situational Analysis of Crime and Deviance. *Annual Review of Sociology*, *19*(1), 114.

Bjerregaard, B. (2000). An Empirical Study of Stalking Victimization. *Violence and Victims*, *15*(4), 389–406.

Bossler, A., & Berenblum, T. (2019). Introduction: New Direction in Cybercrime Research. *Journal of Crime and Justice*. https://doi.org/10.1080/0735648X.2019.1692426

Brantingham, P. L., & Brantingham, P. J. (1991). *Environmental Criminology*. Prospect Heights, Ill.: Waveland Press.

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks and Communications*, *2018*. Retrieved from https://www.hindawi.com/journals/jcnc/2018/1798659/

Breetzke, G. D., & Cohn, E. G. (2013). Burglary in Gated Communities: An Empirical Analysis Using Routine Activities Theory. *International Criminal Justice Review*, *23*(1), 56–74.

Brenner, S. W. (2004). Toward a Criminal Law for Cyberspace : A New Model of Law Enforcement? *Rutgers Computer & Technology Law Journal*, *30*(1), 1–104.

Castells, M. (2002). *The Internet Galaxy : Reflections on the Internet, Business and Society*. Oxford: Oxford Univ. Press.

Center for Strategic and International Studies. (2018). *Economic Impact of Cybercrime - No Slowing Down*.

Chakrabarti, A., & Manimaran, G. (2002). Internet Infrastructure Security: A Taxonomy. *IEEE Network*, *16*, 13–21.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Choi, K. S., & Lee, J. R. (2017). Theoretical Analysis of Cyber-Interpersonal Violence Victimization and Offending Using Cyber-Routine Activities Theory. *Computers in Human Behavior*, Vol. 73, pp. 394–402. https://doi.org/10.1016/j.chb.2017.03.061

Choi, S. (2018). *A Lifestyle-Routine Activity Theory (LRAT) Approach to Cybercrime Victimization: Empirical Assessment of SNS Lifestyle Exposure Activities*. Seoul National University.

Clarke, R. V. G. (1999). *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Coffey, J., Haveard, M., & Golding, G. (2018). A Case Study in the Implementation of a Human- Centric Higher Education Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1).

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization - An Exposition and Test of a Formal Theory. *American Sociological Review*, *46*(5), 505–524.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. Retrieved from https://www.jstor.org/stable/2094589?seq=1#page_scan_tab_contents

Cohen, L. E., Felson, M., & Land, K. C. (1980). Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977; With Ex Ante Forecasts for the Mid-1980s. *American Journal of Sociology*, *86*(1), 90–118.

Conteh, N., & Royer, M. (2016). The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. *International Journal of Computer*, *20*(1), 1–12.

Council of Europe. (2001). *No Convention on Cybercrime*. Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Cross, M., & Shinder, D. L. (2008). *Scene of the Cybercrime* (Vol. 1). https://doi.org/10.1017/CBO9781107415324.004

Cullen, F. T., & Agnew, R. (2006). *Criminological Theory : Past to Present, Essential Readings*. Princeton, N.J.: Roxbury Pub. Co.

Cybersecurity Ventures, & Herjavec Group. (2019). *2019 Official Annual Cybercrime Report*.

de Jong, E., Bernasco, W., & Lammers, M. (2019). Situational Correlates of Adolescent Substance Use: An Improved Test of the Routine Activity Theory of Deviant Behavior. *Journal of Quantitative Criminology*. https://doi.org/10.1007/s10940-019-09433-w

DeGarmo, M. (2011). Understanding the Comparisons of Routine Activities and Contagious Distributions of Victimization: Forming a Mixed Model of Confluence and Transmission. *International Journal of Criminology*, *4*(1), 584–603.

Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, *32*(4), 411–424.

Denning, D. E. R. (1999). *Information Warfare and Security*. Reading, Mass: Addison-Wesley.

Dodge, M., & Kitchin, R. (2003). Mapping Information and Communication Technologies. In *Mapping Cyberspace* (pp. 104–106). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=96104

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach. *Computers in Human Behavior*, *92*, 403–418.

Easterbrook, F. H. (2015). Cyberspace and the Law of the Horse. *The University of Chicago Legal Forum*, *1996*(1).

Eck, J. E., & Clarke, R. V. (2003). Classifying Common Police Problems: A Routine Activity Approach. *Crime Prevention Studies*, *16*, 7–39.

Europol. (2018). *Internet Organised Crime Threat Assessment 2018* (p. 15). p. 15.

Fafinski, S., Dutton, W. H., & Margetts, H. (2010). Mapping and Measuring Cybercrime. *OII Working Paper, 18*, *2*(1), 18–24. Retrieved from https://dx.doi.org/10.2139/ssrn.1694107

Felson, M. (2006). Those Who Discourage Crime. In J. Eck & D. Weisburd (Eds.), *Crime Prevention Studies (Book 4)* (pp. 53–66). Monsey.

Felson, M. (1998). *Crime and Everyday Life: Insights and Implications for Society*. London: Pine Forges Press.

Felson, M., & Boba, R. (2010). *Crime and Everyday Life*. Los Angeles: Sage.

Felson, R. (1996). Big People Hit Little People: Sex Difference in Physical Power and Interpersonal Violence. *Criminology*, *34*(3), 433–452.

Felson, R. (1995). Crime and Everyday Life - Insight and Implications for Society. *Canadian Journal of Criminology*, *37*(2), 263.

Fisher, B. S., Sloan, J. J., Cullen, F. T., & Lu, C. (1998). Crime in the Ivory Tower: The Level and Sources of Student Victimization. *Criminology*, *36*(3), 671–710.

Fisher, B. S., Cullen, F. T., & Turner, M. G. (2002). Being Pursued: Stalking Victimization in A National Study of College Women. *Criminology & Public Policy*, *1*(2), 257–308.

Forester, T., & Morrison, P. (2001). *Computer Ethics : Cautionary Tales and Ethical Dilemmas in Computing*. Cambridge, Mass. [u.a.]: MIT Press.

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy.*, *10*(2), 40–49.

Furnell, S. M. (2002). Categorising Cybercrime and Cybercriminals The problem and potential Approaches. *Journal of Information Warfare*, *1*(2), 35–44.

García-Segura, L. (2020). European Cybersecurity: Future Challenges from a Human Rights Perspective. In J. Ramírez & J. Biziewski (Eds.), *Advanced Sciences and Technologies for Security Applications*. Springer.

Ghernaouti, S., & Simms, D. (2014). *A Report on Taxonomy and Evaluation of Existing Inventories*. Retrieved from www.ecrime-project.eu

Girasa, R. J. (2002). *Cyberlaw: National and International Perspectives*. Upper Saddle River, N.J.: Prentice Hall.

Goodman, M. D. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law and Technology*, *10*, 465–494.

Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, *10*, 139–223.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*. https://doi.org/10.1007/s11416-006-0015-z

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, *10*(2), 243–249.

Grabosky, P., & Smith, R. (2001). Telecommunication Fraud in the Digital Age: The Convergence of Technologies. In *Crime and the Internet*. United Kingdom.

Grabosky, P. (2001). Computer Crime: A Criminological Overview. *Forum on Crime and Society*, *1*(1), 35–53.

Grzybowski, M. K. (2012). *An Examination of Cybercrime and Cybercrime Research: Self-Control and Routine Activity Theory*. Arizona.

Hansman, S., & Hunt, R. (2005). A Taxonomy of Network and Computer Attacks. *Computers and Security*, *24*(1), 31–43.

Hawley, A. H. (1950). *Human Ecology: A Theory of Community Structure*. New York: The Ronald Press Company.

Henney, M. (2018). Chinese Theft of US Intellectual Property 'Greatest Transfer of Wealth' in History.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge Mass: Ballinger Publ.

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for Crime Prevention: A Critical Review of the Literature. *Crime, Law and Social Change*, *56*(1), 53–70. https://doi.org/10.1007/s10611-011-9309-2

Holt, T. J., & Bossler, A. M. (2009). Examining The Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/http://dx.doi.org.ezproxy.uky.edu/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4). https://doi.org/http://dx.doi.org/10.1177/1043986213507401

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework. *International Journal of Offender Therapy and Comparative Criminology*, *62*(6), 1720–1741. https://doi.org/10.1177/0306624X16679162

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low Self-Control, Ractivities, And Fraud Victimization. *Criminology*, *46*(1), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Hootsuite, & We Are Social. (2019). Digital 2019. Retrieved from https://es.slideshare.net/DataReportal/digital-2019-argentina-january-2019-v01?from_action=save

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648X.2019.1691859

Ibrahim, S. (2016). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ilievski, A. (2016). An Explanation of the Cybercrime Victimisation: Self-Control and Lifestyle/Routine Activity Theory. *Innovative Issues and Approaches in Social Sciences*, *9*(1), 30–47. https://doi.org/10.12959/issn.1855-0541

Ingraham, D. (1980). On Charging Computer Crime. *The John Marshall Journal of Information Technology & Privacy Law*, *2*(1).

Jalkanen, J. (2019). *Is Human the Weakest Link in Information Security?: A Systematic Literature Review*. University of Jyvaskyla.

Kanellis, P., Kiountouzis, E., & Kolokotronis, N. (2006). *Digital Crime and Forensic Science in Cyberspace* (P. Kanellis, Ed.). Hershey, PA: Idea Group Inc (IGI.

Kirwan, G., & Power, A. (2014). *Psychology of Cyber Crime: Concepts and Principles.* Hershey: IGI Global.

Kitchin, R. (1998). Towards Geographies of Cyberspace. *Progress in Human Geography*, *22*(3), 385–406. Retrieved from http://eprints.maynoothuniversity.ie/3919/1/RK_cyberspace.pdf

Koenig, D. (2002). Investigation of Cybercrime and Technology-related Crime. Retrieved November 1, 2017, from http://neiassociates.org/cybercrime-and-technology

Kokkinos, C. M., & Saripanidis, I. (2017). A Lifestyle Exposure Perspective of Victimization Through Facebook Among University Students. Do Individual Differences Matter? *Computers in Human Behavior*, *74*, 235–245.

Kringen, J. A., & Felson, M. (2014). Routine Activities Approach. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 4544–4551). https://doi.org/10.1007/978-1-4614-5690-2_586

Krone, T. (2005). *High Tech Crime Brief: Hacking Motives*. Retrieved from http://www.aic.gov.au/publications/htcb/htcb006.html

Kunz, M., & Wilson, P. (2004). *Computer Crime and Computer Fraud*. University of Maryland.

Land, L., Smith, S., & Pang, V. (2013). Building a Taxonomy for Cybercrimes. *Pacific Asia Conference on Information Systems.*

Lattimer, C. (2013). The Future of Geospatial Technologies in Securing Cyberspace.

Lee, J., & Downing, S. (2019). An Exploratory Perception Analysis of Consensual and Nonconsensual Image Sharing. *Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 23–43.

Lee, M., & Alshalan, A. (2005). Geographic Variation in Property Crime Rates: A Test of Opportunity Theory. *Journal of Crime and Justice*, *28*(2), 101–127.

Lee, S.-S., Choi, K., Choi, S., & Englander, E. (2019). A Test of Structural Model for Fear of Crime in Social Networking Sites. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 5–22.

Lessig, L. (2008). *Code and Other Laws of Cyberspace, Version 2.0.* Retrieved from http://bangor.eblib.com/patron/FullRecord.aspx?p=903037

Leukfeldt, E. R. (2017). *Research Agenda The Human Factor in Cybercrime and Cybersecurity.*

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Lewis, B. C. (2004). Prevention of Computer Crime Amidst International Anarchy. *The American Criminal Law Review*, *41*(3), 1353–1372.

Lewis, J. (2018). *Economic Impact of Cybercrime - No Slowing Down*. Santa Clara.

Louderback, E. R., & Roy, S. S. (2018). Integrating Social Disorganization and Routine Activity Theories and Testing the Effectiveness of Neighbourhood Crime Watch Programs: Case Study of Miami-Dade County, 2007-15. *British Journal of Criminology*, *58*(4), 968–992.

Madriaza, P., & Palacio, A. de. (2018). *Crime Prevention and Community Safety : Preventing Cybercrime*. Retrieved from https://www.deslibris.ca/ID/10099197

Malby, S. (2013). *Comprehensive Study on Cybercrime.* Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unodc-comprehensive-study-cybercrime

Marcum, C. (2008). Identifying Potential Factors of Adolescent Online Victimization in High School Seniors. Retrieved from http://libres.uncg.edu/ir/asu/f/Marcum_CD_2008_Identifying_Potential.pdf

Marcum, C. (2011). Adolescent Online Victimization and Constructs of Routine Activities Theory. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. 253–276).

Marcum, C., Ricketts, M., & Higgins, G. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review*, *35*(4), 412–437.

McGuire, M. (2007). *Hypercrime: A Geometry of Virtual Harm.* Retrieved from http://site.ebrary.com/id/10205605

McGuire, M., & Dowling, S. (2013). *Cyber Crime: A Review of the Evidence.*

Mendez, F. (2005). The European Union and Cybercrime: Insights from Comparative Federalism. *Journal of European Public Policy*, *12*(3), 509–527.

Messner, S. F., & South, S. J. (1992). Interracial Homicide: A Macrostructural-Opportunity Perspective. *Official Journal of the Eastern Sociological Society*, *7*(3), 517–536.

Messner, S. F., & Tardiff, K. (1985). The Social Ecology of Urban Homicide: An Application of the Routine Activities Approach. *Criminology*, *23*(2), 241–267.

Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009). *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*. Retrieved from http://www.osti.gov/servlets/purl/967712-BNpjlx/

Miethe, T. D., & Meier, R. F. (1994). *Crime and its Social Context: Toward an Integrated Theory of Offenders, Victims, and Situations*. Albany: State University of New York Press.

Mihalache, A. (2002). *The Cyber Space – Time Continuum : Meaning*. (November 2001), 293–301. https://doi.org/10.1080

Miller, J. M., Schreck, C. J., & Tewksbury, R. A. (2006). *Criminological Theory: A Brief Introduction*. Princeton, NJ: Recording for the Blind & Dyslexic.

Miró-Llinares, F. (2014). Routine Activity Theory. *The Encyclopedia of Theoretical Criminology*, (1979), 1–7. https://doi.org/10.1002/9781118517390/wbetc198

Mohanty, S., Ganguly, M., & Pattnaik, P. (2018). CIA Triad for Achieving Accountability in Cloud Computing Environment. *The Things Services and Applications of Internet of Things*, 39–44. https://doi.org/2321-8363

Moise, A. C. (2014). Some considerations on the phenomenon of cybercrime. *Journal of Advanced Research in Law Economics*, *1*(9), 38–43. https://doi.org/10.14505/jarle.v5.1(9).04

Moitra, S. D. (2005). Developing Policies for Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice*, *13*(3), 435–464.

Moore, R., Guntupalli, N., & Lee, T. (2010). Parental Regulation and Online Activities: Examining Factors that Influence a Youth's Potential to Become a Victim of Online Harassment. *International Journal of Cyber Criminology*, *4*, 685–698.

Moore, R. (2011). *Cybercrime: Investigating High-Technology Computer Crime*.

Mossberger, K., Tolbert, C. J., & Stansbury, M. (2003). *Virtual Inequality: Beyond the Digital Divide*. Washington (D.C.): Georgetown University Press.

Navarro, J. N., & Jasinski, J. L. (2012). Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum*, *32*(1), 81–94.

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber Crime Victimization Among Internet Active Nigerians: An Analysis of Socio- Demographic Correlates. *International Journal of Criminal Justice Sciences*, *8*(2), 225–234.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton: Willan.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology*. https://doi.org/10.5281/zenodo.495762

Nurse, J. (2018). *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*. Oxford University Press.

Oksanen, A., & Atte, K. (2013). Young People as Victims of Crime on the Internet: A Population-Based Study in Finland. *Vulnerable Children and Youth Studies*, *8*(4), 298–309. Retrieved from http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=psyc10&NEWS=N&AN=2013-38377-003

Petrossian, G. A., & Clarke, R. V. (2014). Explaining and Controlling Illegal Commercial Fishing: An Application of the CRAVED Theft Model. *British Journal of Criminology*, *54*, 73–90.

Piper, T. (2019). *An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical*. SANS Institute.

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology*, *21*(1), 55–71.

Ponemon Institute, & Accenture Security. (2019). *Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection*.

Poonia, A. (2014). Cyber Crime: Challenges and Its Classification. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(6), 119–121.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-Control and Victimization: A Meta-Analysis. *Criminology*, *52*(1), 87–116.

Press, R. M. (2016). *Peaceful Resistance: Advancing Human Rights and Democratic Freedoms*. Retrieved from https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc_100041341140.0x000001

Press, S. J. (2003). Subjective and Objective Bayesian Statistics: Principles, Models and Applications. *Wiley Series in Probability in Statistics*. https://doi.org/10.1017/CBO9781107415324.004

Rechavi, A., Berenblum, T., Maimon, D., & Sevilla, I. (2015). Hackers Topology Matter Geography. *Advances in Social Networks Analysis and Mining 2015 (ASONAM)*. New York, NY.

Ren, F., Kwan, M.-P., & Schwanen, T. (2013). Investigating the Temporal Dynamics of Internet Activities. *Time & Society*, *22*(2), 186–215.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

Reyns, B. W. (2015). A Routine Activity Perspective on Online Victimisation. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2018). *Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?* https://doi.org/10.1007/s12103-018-9447-5

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Rogers, M. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*.

Rogers, M. (1999). *Modern-Day Robin Hood or Moral Disengagement: Understanding the Justification for Criminal Computer Activity*.

Rogers, M. K., Seigfried, K., & Tidke, K. (2006). Self-Reported Computer Criminal Behavior: A Psychological Analysis. *Digital Investigation Digital Investigation*, *3*, 116–120.

Rogin, J. (2012). NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History."

Rosenzweig, P. (2013). Thinking About Cybersecurity: From Cyber Crime to Cyber Warfare. Retrieved from www.thegreatcourses.com

Rosenzweig, P. (2013). *Cybersecurity, an Introduction*. Retrieved from http://paulrosenzweigesq.com/media_cybersecurity.php

Rountree, P. W., Land, K. C., & Miethe, T. D. (1994). Macro-Micro Integration in the Study of Victimization: A Hierarchical Logistic Model Analysis Across Seattle Neighborhoods. *Criminology*, *32*(3), 387–414.

Roy, M. (2019). Forcepoint Pushes "Human-Centric Cybersecurity" Approach. Retrieved December 30, 2019, from TechTarget website: https://searchsecurity.techtarget.com/news/252461994/Forcepoint-pushes-human-centric-cybersecurity-approach

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super Controllers and Crime Prevention: A Routine Activity Explanation of Crime Prevention Success and Failure. *Security Journal*, *23*(1), 37–51.

Saravanan, M., & Thilagaraj, R. (2014). Cyber Crime Spatial Data Analysis. *International Journal of Applied Sciences and Engineering Research*, *3*(2). https://doi.org/10.6088/ijaser.030200015

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to Cybercrime: Current Trends. *Police Practice and Research*, *19*(6), 515–518.

Schreck, C., & Fisher, B. (2004). Specifying the Influence of Family and Peers on Violent Victimization: Extending Routine Activities and Lifestyles Theories. *Journal of Interpersonal Violence*, *19*(9), 1021–1041.

Schwab, K. (2019). *The Global Competitiveness Report 2019*. Cologny/Geneva.

Shinder, D. (2011). What Makes Cybercrime Laws so Difficult to Enforce. Retrieved December 31, 2019, from TechRepublic website: https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/

Smith, C. B., McLaughlin, M. L., & Osborne, K. K. (2006). Conduct Control on Usenet. *Journal of Computer-Mediated Communication*, *2*(4), 0.

Smith, M. (1999). Invisible Crowds in Cyberspace. In *Communities in Cyberspace* (pp. 195–219). London: Routledge.

Smith, M. A., & Kollock, P. (1999). *Communities in Cyberspace*. London; New York: Routledge.

Somer, T. (2019). Taxonomies of Cybercrime: An Overview and Proposal to be Used in Mapping Cybercriminal Journeys. *18th European Conference on Cyber Warfare and Security*. Chester.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization. *American Journal of Criminal Justice*, *41*(3), 583–601. https://doi.org/10.1007/s12103-015-9308-4

Stalder, F. (1998). The Logic of Networks: Social Landscapes Vis-a-Vis the Space of Flows'. Retrieved July 13, 2017, from Ctheory website: https://journals.uvic.ca/index.php/ctheory/article/view/14884/5779

Stein, R. E. (2011). *The Contextual Variation of Routine Activities : A Comparative Analysis of Assault Victimization*. *1*(10), 11–24.

Sukhai, N. (2004). Hacking and Cybercrime. In ACM Press (Ed.), *1st Annual Conference on Information Security Curriculum Development,*. Kennesaw, Georgia.

Tavani, H. T. (2011). *Ethics and technology: Controversies, Questions and Strategies for Ethical Computing*. Hoboken, N.J.: Wiley.

Tavani, H. T. (2001). The State of Computer Ethics as a Philosophical Field of Inquiry: Some Contemporary Perspectives, Future Projections and Current Resources. *Ethics and Information Technology*, *3*(2), 97–108.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2018). *Digital Crime and Digital Terrorism*.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, *33*(5), 890–911.

Tewksbury, R., & Mustaine, E. E. (2003). College Students' Lifestyles and Self-Protective Behaviors: Further Considerations of the Guardianship Concept in Routine Activity Theory. *Criminal Justice and Behavior*, *30*, 302–327.

Thomas, D. (2006). An Uncertain World. *The British Computer Society*, *48*(5), 12–13.

Tillyer, M. S., & Eck, J. E. (2009). Routine Activities. In *21st century criminology: A Reference Handbook* (pp. 279–287). Thousand Oaks, CA: Sage Publications.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary Victimization in England and Wales, the United States and the Netherlands. *British Journal of Criminology*, *44*(1), 66–91.

United Nations Conference on Trade and Development. (2019). Digital economy report. *Digital Economy Report*.

United Nations Office on Drugs and Crime. (2018). Structural Factors and Organized Crime. Retrieved January 20, 2020, from The Doha Declaration: Promoting a Culture of Lawfulness website: https://www.unodc.org/e4j/en/organized-crime/module-6/key-issues/structural-factors.html

United Nations Office on Drugs and Crime. (2019). Obstacles to Cybercrime Investigations. Retrieved December 29, 2019, from The Doha Declaration: Promoting a Culture of Lawfulness website: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html

Urbas, G., Choo, K.-K. R., & Criminology., A. I. of. (2008). *Resource Materials on Technology-Enabled Crime*. Retrieved from http://www.aic.gov.au/publications/tbp/tbp028

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 1–20. https://doi.org/10.1177/1043986215621379

van Wilsem, J. (2013). "Bought it, but Never Got it" Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178.

van Wilsem, J. (2011). Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization. *European Journal of Criminology*, *8*(2), 115–127.

van Wilsem, J. (2013). Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453. https://doi.org/10.1177/1043986213507402

Wall, D. (2007). *Cybercrime : The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

Wall, D. (2001). Cybercrimes and the Internet. In *Crime and the Internet*. United Kingdom.

Wall, D. S. (2005). *The Internet as a Conduit for Criminal Activity*. 77–98.

Wikstrom, R. (2018). *The Evolution of Technology*. Retrieved from https://www.overdrive.com/search?q=15784FFE-6257-49A9-B59B-D5AECC22BD20

Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism : Vulnerabilities and Policy Issues for Congress*. Retrieved from http://www.fas.org/sgp/crs/terror/RL32114.pdf

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2007). Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses. *Social Science Computer Review*, *26*(3), 317–333.

Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M. (2006). *Cybercrime and Society*. London: Sage Publications.

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories* (Kent State University). Retrieved from http://rave.ohiolink.edu/etdc/view?acc_num=kent1279290984.